

UNITED STATES DISTRICT COURT

for the
Western District of Oklahoma

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Black TDS WiFi Modem

Case No. 24-MJ-146-STE

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A, which is attached and incorporated by reference.

located in the Western District of Oklahoma, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, which is attached and incorporated by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

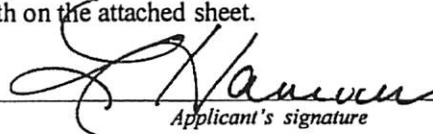
Code Section	Offense Description
18 U.S.C. § 2252A(a)(5)(B)	Possession of Child Pornography
18 U.S.C. § 2252A(a)(2)	Receipt and/or Distribution of Child Pornography

The application is based on these facts:

See attached Affidavit of Special Agent Elizabeth Hancock.

☐ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

Elizabeth Hancock, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date:

Feb 16, 2024


Judge's signature

City and state: Oklahoma City, Oklahoma

SHON T. ERWIN, U.S. MAGISTRATE JUDGE

Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Elizabeth Hancock, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a “federal law enforcement officer” within the meaning of Federal Rule of Criminal Procedure 41(1)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. I am commissioned as a Special Agent (SA) with Immigration and Customs Enforcement (ICE) HSI in Oklahoma City, Oklahoma, and have been so employed by HSI since August 2019. In securing said commission, I received formal law enforcement training, to include over 23 weeks at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia, as it pertains to investigating and enforcing violations of Federal law, including violations of Federal customs and smuggling statutes, as well as child exploitation crimes.

2. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for items specifically described in Attachment A of this Affidavit (hereinafter referred to as the “**TARGET DEVICES**”), which are stored at 3625 NW 56th Street in Oklahoma City, Oklahoma 73112, for evidence that constitutes: evidence of the commission of a criminal offense; contraband, the fruits of crime, and things otherwise criminally possessed; and property designed and intended for use, and which has been used as a means of committing criminal offenses, namely, violations of 18 U.S.C. § 2252A(a)(5)(B), Possession of Child Pornography; and 18 U.S.C. § 2252A(a)(2) Receipt and/or Distribution of Child Pornography. As set forth below, I have probable cause to believe that such property and items, as described in Attachment B, will contain evidence of the described offenses.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

4. The facts in this Affidavit come from my personal observations, my training and experience, and information obtained from other agents, law enforcement personnel, written reports, and surveillance conducted. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included every fact known to me concerning this investigation. I have set forth only the facts that are necessary to establish probable cause that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A(a)(5)(B), Possession of Child Pornography, and 18 U.S.C. § 2252A(a)(2), Receipt and/or Distribution of Child Pornography, by Jimmy Pierce will be located in the **TARGET DEVICES**.

DEFINITIONS

5. The following definitions apply to this Affidavit and Attachment B:

- a. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors in sexually explicit poses or positions.
- b. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is

indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

- c. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such devices: and includes smartphones, and mobile phones and devices.” *See* 18 U.S.C. § 1030(e)(1).
- d. “Computer hardware,” as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input-output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).
- e. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of

hardware, software, or other programming code. A password, a string of alpha-numeric characters, usually operates what might be termed a digital key to “unlock” data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

- f. “Internet Protocol address,” or “IP address,” as used herein, refers to a unique number used by a computer or other digital device to access the Internet. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigned a user’s computer a particular IP address that is used each time the computer accesses the Internet.
- g. “Internet Service Providers” (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.
- h. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

- i. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.
- j. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons or the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.
- k. A “storage medium” is any physical object upon which computer data can be recorded. Examples include hard disks; RAM; “thumb,” “jump,” or “flash” drives; CD/DVDS/ and other magnetic or optical media.
- l. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether stored in a permanent format.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a)(b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States ... that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

7. On February 2, 2024, I, SA Hancock, traveled to the Comanche County Sheriff's Department (CCSD) regarding a child exploitation case the Department was currently investigating. I met with Lieutenant Duran and Detective Bearden and received the following information from them.

8. On January 15, 2024, Meta Platforms, Inc. provided the National Center for Missing and Exploited Children (NCMEC) a CyberTip Report, number 184600876, that detailed information of suspected child pornography being uploaded through the social media platform Facebook, which is owned and operated by Meta Platforms, Inc. The following images were reported to have been uploaded through the social media site:

- a. E7rxblGy0UOGmPxr3761194911_164101403404296_697659540853227
7376_n.jpg
- b. euvaTDMEIq9Rm6Cc412657641_283702767687013_514787575846862
5037_n.jpg
- c. ulWgf20gbWSQBybh413955161_277321185037522_2299224843446267
94_n.jpg

9. Detective Bearden stated one of the images she observed above was of a prepubescent female child sitting with her legs spread toward the camera. A transparent balloon was between the child's spread legs, and the viewer of the image could observe that the child was not wearing underwear, exposing her vaginal area to the camera.

10. The three images above were uploaded on January 12, 2024, by user account number 10094133112966. Detective Bearden completed a search warrant on January 18, 2024, for the subscriber information and account information regarding the user of account number

10094133112966. The return for information from Met Platforms, Inc. showed the username to be “Ok Lahoma” with an attached telephone number of (580) 919-7567. Further investigation of the information returned by Meta Platforms, Inc. showed a post from account number 10094133112966 to another unknown individual on Facebook, which stated something to the effect of, “My name is Jim and I would like more i[n]fo please.”

11. Law enforcement inquiries of the telephone number above resulted in the number being attached to a Sex Offender registration form belonging to Jimmy **PIERCE**. In 2023, **PIERCE** was convicted of Indecent Exposure in Elgin, Oklahoma for taking a digital image of his exposed penis at an elementary school he worked at as a janitor.

12. Registration information showed **PIERCE** registered a home address at 802 1st Street in Elgin, Oklahoma. Upon reviewing the Comanche County Assessor’s site, law enforcement found that the residential address of 802 1st Street was an invalid address. However, by conducting a sex offender compliance check for **PIERCE**, law enforcement confirmed he was living at 800 1st Street in Elgin, Oklahoma.

13. On February 9, 2024, HSI accompanied law enforcement officers from CCSD, as well as Agents with the Oklahoma State Bureau of Investigations (OSBI) to execute a state residential search warrant for the residence(s) located at 800 1st Street in Elgin, Oklahoma. Upon making contact with **PIERCE** at his residence, **PIERCE** told entering officers that he needed to use the restroom before coming outside. While walking to the back bedroom where the bathroom was located, **PIERCE** was observed to attempt to take his cell phone with him. He was ordered by law enforcement to leave his phone.

14. The following items, collectively referred to as the **TARGET DEVICES**, were seized and taken into custody by law enforcement upon execution of the residential search warrant for **PIERCE**'s home, located at 800 1st Street, Elgin, Oklahoma:

- a. (1) Asus laptop computer;
- b. (1) Blue HP laptop computer;
- c. (1) Defender Connected surveillance hard drive;
- d. (1) Black TDS WiFi Modem;
- e. (1) Black Samsung cell phone bearing International Mobile Equipment Identification (IMEI) number 352574701216846;
- f. (1) Black Samsung cell phone bearing IMEI number 352678734186122;
- g. (1) Silver LG smartphone; and
- h. (1) Kodak PixPro AZ255 digital camera.

15. OSBI Agents were able to preview the cell phone **PIERCE** attempted to take to the bathroom, which was later identified as a black Samsung cellular telephone Model SM-S146VL (GP), International Mobile Equipment Identity (IMEI) number 352678734186122, one of the **TARGET DEVICES**. A review of the cell phone resulted in there being numerous videos and images of child pornography located on the cell phone, including the following described videos, which I observed on scene during the preview:

- a. One (1) video of a prepubescent female wearing no clothing, lying on her back. The child is observed to have her legs completely spread, exposing her vaginal area. The child is observed to urinate toward the camera.
- b. One (1) video of a prepubescent female wearing a white tank top pulled up over her chest, exposing her chest area. She is not wearing any underwear

or bottoms, exposing her vaginal area. The child is also lying on her back, and she is wearing a purple mask covering the majority of her face. An unknown male wearing no bottoms is observed to enter the frame of the camera. This man then begins to vaginally sexually assault the child using his penis.

16. I, along with Detective Bearden, conducted an interview with **PIERCE**. Post-*Miranda*, **PIERCE** admitted to downloading and trading child pornography utilizing social media sites. **PIERCE** stated he has been utilizing the Internet to download and trade such images and videos for approximately two years and has been viewing child pornographic material for a decade or more.

17. **PIERCE** stated law enforcement would “probably” find child pornography images and videos on the other two cell phones found at the house.

18. With respect to the laptops seized from the house, **PIERCE** indicated that both he and his wife used them and that they would not contain child pornography. **PIERCE** stated only his cell phones could contain child pornography. However, based on my training and experience, I know that child pornography collectors are not always honest about the locations in which they keep child pornography.

CHARACTERICS COMMON TO CHILD PORNOGRAPHY COLLECTORS

19. As a result of my consultations with other law enforcement officers, both federal and state, who have considerable experience investigating the sexual exploitation of children, and my own experience, I have learned about the individuals engaged in child exploitation activities and about the computer technology available to, and utilized by, those individuals. I have learned

that individuals engaged in the production, procurement, trade, and/or transmission of child exploitation through the United States mail, computer, or other interstate conveyance commonly:

- a. Receive sexual gratification and satisfaction from actual physical contact with children and from fantasy that may be simulated by producing and viewing children engaged in sexual activity or in sexually suggestive poses.
- b. Own and operate photographic production and reproduction equipment. This equipment is often digital cameras which include both camera which take still images and movie files.
- c. Collect sexually explicit or suggestive materials of adults and/or children consisting of photographs, magazines, motion pictures, videotapes, books, slides, computer images, drawings or other visual media for their own sexual arousal and gratification, and in some instances, to lower the inhibitions of children they are attempting to seduce, and/or to arouse and to demonstrate their desired sexual acts to their selected partners or victims.
- d. Often do not dispose of their collection of sexually explicit material. If the material is discarded or lost due to computer malfunction, these individuals often replenish their supply of child exploitation materials very quickly.
- e. Correspond with individuals who share their same interest in child exploitation materials, and maintain their names, addresses, telephone numbers, and other identifying information in lists, telephone books, address books, scraps of paper, or on computer disks.
- f. Obtain, collect, and maintain photographs of children they are or have been involved with, which may depict children fully clothed, in various states of

undress, totally nude, or in various activities, which are often held for lengthy periods of time.

- g. Collect books, magazines, newspapers, and other writings about sexual assaults of children to understand their own feelings toward children, to justify their feelings, and to find countenance for their illicit behaviors and desires.
- h. Commonly collect items which could be any material relating to children that serve a sexual purpose for a given individual. These items as used herein, have been termed “child erotica” and so defined by now retired Special Agent Ken Lanning, Federal Bureau of Investigation. *See* Kenneth Lanning, *Child Molesters: A Behavioral Analysis* (2001) at page 65. Some of the more common types of “child erotica” include photographs that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids. Federal courts have recognized the evidentiary value of child erotica and its admissibility in child exploitation cases. *United States v. Riccardi*, 258 F.Supp.2d 1212 (D. Kan. 2003); *United States v. Caldwell*, 181 F.3d 104 (6th Cir. 1999) (unpublished) (child erotica admissible under Federal Rules of Evidence 404(b) to show knowledge or intent).
- i. Often do not discard the child exploitation material but collect it over a long period of time and maintain this material in the privacy of their homes. Sometimes, individuals using peer-to-peer software will engage in a routine where they may delete their child exploitation material after they have viewed it several times and then, after the deletion occurs, the individual

will replenish their supply via their peer-to-peer connection when they desire more images to satisfy their sexual interest in children. This procurement and purging cycle results in evidence of their current child exploitation materials being easily located on their computer, as well as evidence of their deleted material remaining on their computer, which can be recovered by a forensic computer examiner.

- j. In my experience and that of other law enforcement agents with experience investigating child exploitation crimes, individuals who trade and share child exploitation material via the Internet retrieve and store the child exploitation materials (whether they produced it or obtained it from other sources) on an electronic storage device as previously stated. As also previously stated, individuals who trade and share child exploitation materials tend to retain their collection of child exploitation materials on digital media (such as hard drives, computer and/or cell phones), which can be stored for a very long amount of time, and tend to keep their collection nearby and secured, usually within their residence or on their person. It is well-known that when individuals relocate from one residence to another, they take their valued possessions (such as vehicles, furniture, clothes, important documents, computers, electronic devices, etc.) with them and store them in their new residence.

20. Based on the facts set forth above, I believe **PIERCE** engaged in the above-described illegal activities and that a search of the **TARGET DEVICES** will result in the discovery child pornography and related evidence.

COMPUTERS, THE INTERNET, AND CHILD EXPLOITATION

21. I have had training and experience in the investigation of computer-related crimes.

Based on my training, experience, and knowledge, I know the following:

- a. Computers and digital technology have dramatically changed the way in which individuals interested in child exploitation interact with each other. Computers basically serve four functions in connection with child exploitation: production, communication, distribution, and storage.
- b. Individuals involved in child exploitation can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras and smartphones with cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera or smartphone to the computer. In the last ten years or more, the resolution of pictures taken by digital cameras and smartphones has increased dramatically, meaning that such pictures have become sharper and crisper. Photos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards often store up to 256 gigabytes of data, which provides enough space to store thousand of high-resolution photographs and videos. Video camcorders, which once recorded video onto tape or mini-CDs, now can

save video footage in a digital format directly to a hard drive in the camera.

The video files can be easily transferred from the camcorder to a computer.

- c. A device known as a modem allows any computer to connect to another computer using telephone, cable, or wireless connection. Electronic contact can be made to millions of computers around the world. The ability to produce child exploitation images/videos easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child exploitation images/videos. Child exploitation can be transferred via electronic mail or through file transfer protocols (FTP's) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "instant messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child exploitation materials.
- d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child exploitation materials. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. Given the storage capabilities, modern computers can retain many years' worth of a user's data, stored indefinitely. Even deleted data can often be forensically recovered. In addition, there are numerous options available for the storage

of computer or digital files. One-terabyte external and internal hard drives are not uncommon.

- e. Other media storage devices include CDs, DVDs, and “thumb”, “jump”, or “flash” drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or “burn” files onto them).
- f. Some media storage devices can easily be concealed and carried on an individual’s person. Smartphones and/or mobile phones are also often carried on an individual’s person or their immediate vicinity. Digital files can be quickly and easily transferred back and forth between computers (as broadly defined in 18 U.S.C. § 1030(e)) and other digital file storage devices or stored simultaneously on them. For example, smartphones can often sync with a traditional desktop or laptop computer. This can result in files being transferred from the smartphone to the computer or even stored on both devices simultaneously.
- g. The Internet affords individuals several different venues for obtaining, viewing, and trading child exploitation materials in a relatively secure and anonymous fashion. For example, distributors of child exploitation

materials can use membership-based/subscription-based Web sites to conduct business, allowing them to remain relatively anonymous.

- h. Individuals also use online resources to retrieve and store child exploitation materials, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides email services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child exploitation can be found on the user's computer or external media in most cases.
- i. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (i.e., by saving an email as a file on the computer or saving the locations of one's favorite websites in, for example, "bookmarked" files). Digital information can also be retained unintentionally such as the traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data. Accordingly, a computer forensic examiner can often find

evidence of deleted files on a user's computer. Thus, if a user has downloaded image files, viewed them, then deleted them, a computer forensic examiner could oftentimes find evidence of such actions and maybe even the deleted images themselves.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

22. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on devices. This information can sometimes be recovered with forensics tools.

23. I know that cellular telephones are often equipped with digital cameras and those phones possess the capability to transmit and/or store electronic images. I know that in many cases, cellular telephones maintain photographs of illegal activities. These photos are sometimes stored in cellular phones and often are transmitted or sent from one electronic media device to another. I also know that cellular phones may contain notes regarding potential illegal acts that are recorded by the subject who possesses the electronics. Furthermore, I know that text messages and emails are often used by two or more persons to communicate information regarding illegal activities, between principals and co-conspirators of those crimes.

24. I know that cellular telephones are utilized by the majority of individuals in the United States and have become a staple of communication between individuals using text messaging, visual and audible communications, as well as applications like Instagram. Additionally, individuals utilize their cellular devices to take and store pictures and keep notes. Communications on phones are kept for long periods and transferred from one phone to another when replaced. This is done through the use of Cloud storage and direct transfer conducted at the

time of purchase or by the individual themselves. Individuals utilize this method as not to lose data that is stored on the phone such as contacts, photos, notes, and other important information to the individual.

25. Cellular telephones are often used to facilitate offenses and allow criminals to maintain communication with each other before, during, and after the commission of offenses. I am aware that cellular telephones have the capacity to store a vast amount of information, including but not limited to: telephone numbers, voice messages, text messages, e-mail, photographs, videos, address books, records, phone call histories, contact and other information.

26. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the offenses noted above, but also forensic evidence that establishes how each of the **TARGET DEVICES** was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on any of the **TARGET DEVICES** because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to

draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

27. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of each of the **TARGET DEVICES** consistent with the warrant. The examination may require authorities to employ techniques (including but not limited to computer-assisted scans of the entire medium) that might expose many parts of the **TARGET DEVICES** to human inspection in order to determine whether they contain evidence described by the warrant.

28. *Manner of execution.* Because this warrant seeks only permission to examine the **TARGET DEVICES** already in law enforcement's possession, the execution of this warrant does

not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause to authorize execution of the warrant at any time in the day or night.

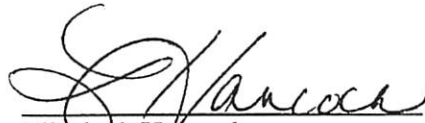
29. *Methods of examination.* In conducting this examination, law enforcement personnel may use various methods to locate evidence and instrumentalities of the crime(s) under investigation, including but not limited to undertaking a cursory inspection of all information within each **TARGET DEVICE**. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with stored cellular device data, such as pictures and videos, do not store as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications associated with a cellular device, as it is impossible to know in advance all of the unique words or phrases investigative subjects will use in their communications. Consequently, often many communications in cellular device data that are relevant to an investigation do not contain any searched keywords.

CONCLUSION

30. Based on the foregoing, there is probable cause to believe that the federal criminal statute(s) cited herein have been violated, and that the contraband, property, evidence, fruits, and instrumentalities of these offenses, more fully described in Attachment B, are located in the **TARGET DEVICES** described in Attachment A. I respectfully request that the Court issue a

search warrant for the **TARGET DEVICES** described in Attachment A, authorizing the search of the items described in Attachment B.

31. I am aware that the recovery of data by a computer forensic analyst take significant time; much the way recovery of narcotics must later by forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the “return” inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by forensic analysts.



Elizabeth Hancock
Special Agent
Homeland Security Investigations

Sworn and subscribed before me this 16th day of February, 2024.



SHON T. ERWIN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF LOCATION(S) TO BE SEARCHED

The Black TDS WiFi Modem that was seized from the residential search of 800 1st Street, Elgin, Oklahoma on February 9, 2024, and which is one of the **TARGET DEVICES**. The **TARGET DEVICES** are presently located at 3625 NW 56th Street in Oklahoma City, Oklahoma 73112.

ATTACHMENT B
ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use, or which is or has been used as the means of committing a criminal offense, namely violations by **Jimmy Pierce** of Title 18, United States Code, Sections 2252A(a)(5)(B) and 2252A(a)(2):

1. Visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or relating to the sexual exploitation of minors or a sexual interest in children.
2. Stories, text-based files, motion pictures, films, videos, and other recordings, or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or relating to the sexual exploitation of minors or a sexual interest in children.
3. Information, correspondence, records, documents, or other materials pertaining to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or pertaining to the sexual exploitation of minors or a sexual interest in children, that were transmitted or received using a computer, cellular device, personal digital assistant, or some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail, including but not limited to:
 - a. Cellular telephones, smartphones, tablets, personal digital assistants, computers, computer systems, computer hardware, computer software, tapes, cassettes, cartridges, streaming tape, commercial software, commercial hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system

disk operating systems, magnetic media floppy disks, tape systems, and other computer related operation equipment;

- b. Digital cameras, scanners, monitors, printers, external storage devices, computer photographs, Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF TIF, AVI, and MPEG), and any electronic data storage devices including, but not limited to hardware, software diskettes, backup tapes, CD-ROMS, DVD, Flash memory devices, and other storage mediums;

4. Envelopes, letters and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors or a sexual interest in children;

5. Books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors or a sexual interest in children;

6. Any and all records, documents, or materials, including any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate commerce including

by United States mail or by computer, any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256 or relating to the sexual exploitation of minors or a sexual interest in children;

7. Any and all records, documents, or materials, including any and all address books, names, and lists of names and addresses of minors visually depicted while engaging in sexually explicit conduct, defined in Title 18, United States Code, Section 2256; or relating to the sexual exploitation of minors or a sexual interest in children;

8. Any and all records of Internet usage including usernames and e-mail addresses and identities assumed for the purposes of communication on the Internet. These records may include billing and subscriber records, chat room logs, e-mail messages, and include electronic files in a computer and on other data storage mediums, including CDs or DVDs;

9. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data; and

10. Files, records, programs, logs, electronic communications, scanning programs, financial records, hacking software, or router configuration software media.

11. Computers or storage media used to commit the violations described above.

12. For any computer or storage medium whose search or seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

- a. Evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords,

documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondences;

- b. Evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. Evidence of the lack of such malicious software;
- d. Evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation, and to the COMPUTER user;
- e. Evidence indicating the COMPUTER user’s knowledge and/or intent as it relates to the crime(s) under investigation;
- f. Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. Evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. Evidence of the times the COMPUTER was used;
- i. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. Documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. Records of or information about Internet Protocol addresses used by the COMPUTER;

- l. Records of or information about the COMPUTER'S Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered in any Internet search engine, and records of user-typed web addresses;
 - m. Contextual information necessary to understand the evidence described in this attachment; and
 - n. Videos/digital images found during the search of the COMPUTER(S), including any of those items saved or taken by or on the COMPUTER(S) searched.
13. Child pornography, as defined as 18 U.S.C. § 2256(8), and child erotica.
14. Records, information, and items relating to violations of the statutes described above, including:
- a. Records, information, and items relating to the use or ownership of the **TARGET DEVICE**.
 - b. Records and information relating to the identity or location of the persons suspected of violating the statutes described above.
 - c. Records and information relating to the sexual exploitation of children, including correspondence and communications between users on the Internet and social media.
 - d. Records and information relating or pertaining to the identity of the person or persons using seized evidence.

As used above, the terms "records" and "information" include all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media

that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro-SD cards, macro-SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.